Amendments to the Claims

Claims 1-4 and 7-20 have been amended. Claims 5, 6, and 21-28 have been canceled. Claims 29, 30, and 31 have been added. The following listing of claims replaces all previous versions of the claims in the application.

Listing of Claims

1. (currently amended) A method for controlling communications in an identity-based encryption (IBE) system in which ~~a message encrypted using an IBE public key of a recipient is to be sent~~ senders communicate with recipients over a communications network ~~from a sender to the recipient, wherein the recipient is in a district associated with an IBE private key generator from which the recipient obtains an IBE private key for decrypting the message encrypted with the IBE public key~~ and in which recipients and IBE private key generators are organized in a plurality of districts, each district including a respective one of the IBE private key generators, wherein the IBE private key generator in each district generates IBE private keys for recipients that are associated with that district, wherein each district has IBE public parameter information that is used by senders in encrypting messages for recipients in that district, wherein each district has district policy information

that includes IBE encryption protocol information, and wherein the recipients in each district use their IBE private keys in decrypting messages that are encrypted using respective IBE public keys, comprising:

~~at the IBE private key generator, providing district policy information to~~ when a sender desires to send a message to a recipient in a given district, obtaining the district policy information for the given district for the sender over the communications network, wherein the district policy information that is obtained for the given district includes IBE encryption protocol information for the given district that specifies an IBE public key format that is to be used in creating IBE public keys for the recipients in the given district; ~~and~~

at the sender, using ~~the district policy information in sending the message to the recipient~~ the IBE public key format specified by the IBE encryption protocol information to construct an IBE public key for the recipient in the given district; and

at the sender, encrypting the message for the recipient using the IBE public parameter information associated with the given district and the IBE public key that has been constructed for the recipient according to the IBE public key format.

2. (currently amended) The method defined in claim 1 ~~wherein using the district policy information at the sender comprises~~ further comprising using the district policy information to determine whether to send the message to the recipient.

3. (currently amended) The method defined in claim 1 ~~wherein using the district policy information at the sender comprises~~ further comprising using the district policy information and client policy information to determine whether to send the message to the recipient.

4 (currently amended) The method defined in claim 1 ~~wherein using the district policy information at the sender comprises~~ further comprising using the district policy information to determine how to send the message to the recipient.

5. canceled

6. canceled

7. (currently amended) The method defined in claim 1 wherein the recipient has a username and wherein the ~~district policy~~ IBE encryption protocol information includes IBE public key format information that specifies which portion of the recipient's username is used to form the IBE public key, the method comprising using the IBE public key format information ~~from the district policy information~~ that specifies which portion of the recipient's username is used to form the IBE public key at the sender to construct the IBE public key from the recipient's username.

8. (currently amended) The method defined in claim 1 wherein the district policy information for the given district includes communications protocol information that specifies which communications protocols are used by the given district, the method comprising using the communications protocol information at the sender to determine which communications protocols are being used by the given district.

9. (currently amended) The method defined in claim 1 wherein the district policy information for the given district includes communications protocol information that specifies which communications protocols are used by the given district, the method comprising using the communications protocol

information at the sender to determine which message format is being used by the given district.

10. (currently amended) The method defined in claim 1 wherein the district policy information includes authentication protocol information that specifies what type of authentication is required before the IBE private key generator for the given district provides IBE private keys to recipients in the given district, the method comprising using the authentication protocol information at the sender in sending the message to the recipient.

11. (currently amended) The method defined in claim 1 wherein the district policy information includes authentication protocol information that specifies what type of authentication is required before the IBE private key generator for the given district provides IBE private keys to recipients in the given district, the method comprising using the authentication protocol information at the sender to determine whether to send the message to the recipient.

12. (currently amended) The method defined in claim 1 wherein the district policy information includes authentication protocol information that specifies what type of authentication

is required before the IBE private key generator for the given district provides IBE private keys to recipients in the given district, the method comprising using the authentication protocol information at the sender to determine whether the recipient uses a smart card when being authenticated by the IBE private key generator.

13. (currently amended) The method defined in claim 1 wherein the district policy information includes content-based protocol information that specifies how messages for recipients in the given district are to be handled based on their content, the method comprising using the content-based protocol information at the sender to determine whether to send the message to the recipient in the given district.

14. (currently amended) The method defined in claim 1 wherein the given district comprises multiple subdistricts, each of the multiple subdistricts having its own respective subdistrict IBE private key generator, wherein the recipient is associated with at least one of the subdistricts, and wherein each subdistrict has associated subdistrict policy information, the method further comprising:

at the sender, obtaining the subdistrict policy information for each of the multiple subdistricts; and

at the sender, using the subdistrict policy information for the multiple subdistricts in sending the message to the recipient.

15. (currently amended) The method defined in claim 1 wherein the given district comprises multiple subdistricts, each of the multiple subdistricts having its own respective subdistrict IBE private key generator, wherein the recipient is associated with more than one of the subdistricts, and wherein each subdistrict has associated subdistrict policy information, the method further comprising:

at the sender, obtaining the subdistrict policy information for each of the multiple subdistricts; and

at the sender, using the subdistrict policy information for the subdistricts with which the recipient is associated in determining which subdistrict to send the message to.

16. (currently amended) The method defined in claim 1 wherein the given district comprises multiple subdistricts, each of the multiple subdistricts having its own respective subdistrict IBE private key generator, wherein the recipient is associated with more than one of the subdistricts, wherein the subdistricts use different techniques for authenticating

recipients, wherein each subdistrict has associated subdistrict policy information that specifies the techniques used for authenticating their recipients, the method further comprising:

at the sender, obtaining the subdistrict policy information for each of the multiple subdistricts; and

at the sender, using the subdistrict policy information for those subdistricts with which the recipient is associated in determining which of those subdistricts to send the message to based on which technique is used to authenticate the recipient at each of those subdistricts.

17. (currently amended) The method defined in claim 1 wherein the message has certain message content ~~and wherein using the district policy information comprises~~, the method further comprising:

at the sender, determining whether to send the message to the recipient based on the message content and the district policy information.

18. (currently amended) The method defined in claim 1 ~~wherein using the district policy information comprises~~ further comprising:

at the sender, using the district policy information to determine whether to display a notice for the

sender.

19. (currently amended) The method defined in claim 1 ~~wherein providing the district policy information to the sender comprises~~ further comprising providing the district policy information to the sender in the form of a district policy information list containing an identifier for each list entry.

20. (currently amended) The method defined in claim 1 ~~wherein providing the district policy information to the sender comprises~~ further comprising providing the district policy information to the sender in the form of a district policy information list having list entries, wherein at least some of the list entries are digitally signed.

21-28. canceled

29. (new) A method for controlling communications in an identity-based encryption (IBE) system in which senders communicate with recipients over a communications network and in which recipients and IBE private key generators are organized in a plurality of districts, each district including a respective one of the IBE private key generators, wherein the IBE private key generator in each district generates IBE private keys for

recipients that are associated with that district, wherein each district has IBE public parameter information that is used by senders in encrypting messages for recipients in that district, wherein each district has district policy information that includes IBE encryption protocol information, and wherein the recipients in each district use their IBE private keys in decrypting messages that are encrypted using respective IBE public keys, comprising:

when a sender desires to send a message to a recipient in a given district, obtaining the district policy information for the given district for the sender over the communications network, wherein the district policy information that is obtained for the given district includes authentication protocol information for the given district that specifies what type of authentication is required before the IBE private key generator for the district provides IBE private keys to recipients in the district;

at the sender, using the authentication protocol information for the given district to determine whether to send the message to the recipient in the given district; and

at the sender, if it is determined that the message is to be sent to the recipient in the given district, encrypting the message for the recipient using the IBE public parameter information associated with the given district and an

IBE public key of the recipient and sending the message to the recipient.

30. (new) A method for controlling communications in an identity-based encryption (IBE) system in which senders communicate with recipients over a communications network and in which recipients and IBE private key generators are organized in a plurality of districts, each district including a respective one of the IBE private key generators, wherein the IBE private key generator in each district generates IBE private keys for recipients that are associated with that district, wherein each district has IBE public parameter information that is used by senders in encrypting messages for recipients in that district, wherein each district has district policy information that includes IBE encryption protocol information, and wherein the recipients in each district use their IBE private keys in decrypting messages that are encrypted using respective IBE public keys, comprising:

when a sender desires to send a message to a recipient in a given district, obtaining the district policy information for the given district for the sender over the communications network, wherein the district policy information that is obtained for the given district includes IBE message format information that specifies at least one IBE message

format that is supported by the given district;

at the sender, using the IBE message format specified by the IBE message format information to construct the message for the recipient in the given district; and

at the sender, encrypting the message for the recipient using the IBE public parameter information associated with the given district and an IBE public key for the recipient and sending the message to the recipient.

31. (new) A method for controlling communications in an identity-based encryption (IBE) system in which senders communicate with recipients over a communications network and in which recipients and IBE private key generators are organized in a plurality of districts, each district including a respective one of the IBE private key generators, wherein the IBE private key generator in each district generates IBE private keys for recipients that are associated with that district, wherein each district has IBE public parameter information that is used by senders in encrypting messages for recipients in that district, wherein each district has district policy information that includes IBE encryption protocol information, and wherein the recipients in each district use their IBE private keys in decrypting messages that are encrypted using respective IBE public keys, comprising:

when a sender desires to send a message to a recipient in a given district, obtaining the district policy information for the given district for the sender over the communications network, wherein the district policy information that is obtained for the given district includes content-based protocol information for the given district that specifies how the given district handles messages depending on their content;

at the sender, using the content-based protocol information for the given district to determine whether to send the message to the recipient in the given district; and

at the sender, if it is determined that the message is to be sent to the recipient in the given district, encrypting the message for the recipient using the IBE public parameter information associated with the given district and an IBE public key of the recipient and sending the message to the recipient.